10 TIPS TO IMPROVE YOUR SECURITY INCIDENT READINESS AND RESPONSE

EXECUTIVE SUMMARY

Information security attacks have become more targeted, more sophisticated, more adaptable and harder to find. As it becomes more difficult to prevent attacks, information security professionals must do a better job responding by reducing attackers’ free time within the network, getting to the root cause faster, and learning from each attack to reduce future risk.

Organizations’ incident readiness and response often falls short in ten areas that span people, processes and technology. By tackling these shortcomings, security professionals can reduce risk by providing early warnings of potential problems, rather than scrambling to chase the latest threat.
10 Tips to Improve Your Security Incident Readiness and Response

A flat security organization reliant only on signature-based security systems aren’t sufficient to address today’s threat environment.

**ARM YOURSELF WITH THE RIGHT STAFF, SKILLS AND TEAM STRUCTURE**

The technology that helps detect, investigate, and respond to security incidents or data breaches is of little use without enough skilled personnel to use it. This staff must have clearly defined roles and responsibilities to ensure consistent, proper responses to threats. End users, meanwhile, need training and encouragement to recognize and avoid phishing and other social engineering threats.

- **Tip 1: Assure adequate staff.** This means at least some staff dedicated to incident response rather than personnel who are part-time or borrowed from other IT or security functions. They should have expertise in areas such as incident detection, forensics, malware analysis, threat intelligence, and breach management. Since most targeted attacks focus on the most popular computing platforms, organizations need at least one staff member capable of both static and dynamic analysis on Windows and x86 architectures. Ideally these would be part of an advanced tools and tactics team, providing advanced support for Level 1 and Level 2 incident response.

A typical staff model might include a threat intelligence analyst, an analysis and tools support analyst, and a Tier 1 and Tier 2 analyst, all reporting to the security operations center manager. Some of these roles can also be filled by service providers or contractors rather than by full-time internal personnel. Each person should receive adequate and ongoing training specific to their role, with regular staff rotation to increase skills and reduce burnout.

- **Tip 2: Clearly define roles and responsibilities.** If everyone in the IT department is a potential incident responder, no one has clear responsibility. This can result in confusion, inconsistent processes and prioritization, and worst of all that nobody responds to an incident because they assume someone else is.

Roles and responsibilities should be clearly defined, differentiating between the management of security devices, the management of incidents, and the management of security data and analysis. Organizations should deploy tiered and specialized staff with the flexibility to quickly ramp up their incident response teams.
Level 1 incident responders should be responsible for service level-driven investigations, based on well-documented processes, procedures and checklists – for example, the completion of all checklist procedures within an allotted timeframe. Level 2 incident responders should be responsible for troubleshooting and correlating data from different sources. For example, a Level 2 analyst may need to combine a log review with a review of issues stemming from packet capture and host systems. The most security mature organizations may add an internal Level 3 team, while less mature organizations may turn to an outsourcer for this capability. This Level 3 team performs malware analytics and reverse engineering that breaks the malware’s machine code back into source code to better identify the specific nature of the attack and how to combat it. By understanding what the malware does and how it works, the analyst will also be better able to defend against variants of the attacker tools, tactics and procedures in the future.

- **Tip 3: Increase user awareness/training for avoiding advanced threats.** End users are often the weakest point in an organization’s defenses, falling victim to techniques such as spear phishing and social engineering that allow attacks into the network. While users may know they should ask for proof before giving their password to someone claiming to call from “the help desk,” it’s easy to forget such guidelines in the press of everyday work.

It’s up to the security staff to find creative ways to make the lessons stick. One approach is to conduct actual internal phishing attacks and publicize to the internal staff how easy or hard it was for the attack to succeed. Creating friendly competition among user departments over which can best see through an attack can encourage attention and compliance.

**BEEF UP YOUR PROCESSES FOR CONTINUOUS IMPROVEMENT**

Most organizations focus only on getting back to normal after an attack, with actions such as reimaging of systems, changing firewall rules and updating IDS/IPS signatures. These do not, however, sufficiently reduce future risks. By defining both high-level objectives and detailed processes and procedures for detecting, responding to and analyzing incidents, an organization can gain clearer and more detailed insights into the incident. This helps them detect, investigate and remediate attacks more rapidly and effectively, and reduce the risk of damage.

- **Tip 4: Formalize response processes and procedures.** In security, as in so many other areas, ad-hoc efforts lead to ad-hoc results, which can leave dangerous gaps in an organization’s defenses. Predefined, monitored, and enforced workflows help assure accountability and consistency, and can be more easily tracked to improve an organization’s security posture over time. When it comes to critical incidents, most organizations take an “all hands on deck” approach and are generally good at fighting fires and containing an incident before anything really bad happens.

An organization is on the road to improved response if it prioritizes incidents to focus the most attention, staff and budget on its highest-value applications and data, as well as those platforms that are most vulnerable to an exploit. The organization has reached an even higher level of maturity if its incident responses are guided by clear governance rules and investigative run books.
Such a run book might include, for example, step-by-step instructions for responses to common events and incidents such as detection of malware, rootkits and rogue wireless devices. Other responses might apply to potentially risky conditions such as unwanted administrative access to executive mailboxes and attempts to access known malware domains. Organizations should leverage industry best practices for incident response procedures, such as those from NIST, VERIS and the SANS Institute. They should also document their own best practice procedures and prepare run books to assure a more consistent response to future incidents.

**Tip 5: Improve vulnerability management.** The move to “bring your own device“, and the use of on-demand cloud platforms by business units unwilling to wait for formal IT procurement processes, makes it harder to find “rogue” IT systems that could pose a security threat.

A review of network traffic will likely reveal unknown systems and unexpected data flows that have bypassed IT asset governance processes. It can also reveal outdated operating systems, browsers and versions of Java that can be exploited in attacks. Vulnerability scans also reveal unpatched and non-compliant configurations that pose security risks. Organizations need to look beyond reports that run thousands or tens of thousands of pages and lack the business context to prioritize which systems are most important to the organization. (See Tip 7 below for details on how to perform such business-centric vulnerability ranking.)

An effective patching process should also assess the risk and cost of each patch. It may include, depending on the criticality of the issue, testing to ensure the patch doesn’t conflict with other elements in the environment. It should also include rollback and recovery procedures in case the patch does cause a service interruption.

**Tip 6: Learn from past incidents and breaches.** Effective incident response improves the organization’s security posture over time. This requires thorough and complete documentation of the incident response both during and after the investigation. (See Tip 7 below for what a security incident response tracking system should contain.) That data should be used to improve the organization’s processes and systems for detecting, investigating and limiting the damage from future incidents. The data should address metrics such as mean time to incident detection and resolution, as well as indicate the general level of effectiveness of existing countermeasures. This enables the organization to determine whether budget is being allocated optimally. Furthermore, those in charge of a Critical Incident Response Center (CIRC) or a Security Operations Center (SOC) need the authority and internal stakeholder support to investigate and respond to incidents as they see fit.

To achieve continued improvement, response processes must be repeatable and measurable through key performance indicators (KPIs) that are relevant to the business. If one KPI is “time to resolution,” the organization’s performance against it can help identify what people, processes or technology helped or stood in the way of reaching that goal. An incident management system can help identify the root cause and set a measurable goal to learn from the past and measure whether and how the response is improving.

More mature organizations also document use cases that describe actual response situations and threat scenarios specific to them. This helps assure that the rest of the team can learn from past incidents and improve their response.
What We Need
Intelligence-driven Model for Incident Response

A coordinated, centralized and trackable intelligence-driven process, backed by skilled staff and the right technology, enables continual improvement and reduced risk from security incidents.

- **Controls**: the ability to get the right data from the right controls, both signature-based and signature-less.
- **Context**: the fusion of controls data with business, threat and risk context in order to determine incident priority.
- **Visibility**: the aggregation of Controls and Context and the ability to manage incidents within a “single pane of glass.”
- **Expertise**: the training, skills and experience of the team responsible for defending the organization and managing the solution set.

UPGRADE YOUR MONITORING AND ANALYSIS SYSTEMS

Today’s information systems, and the attacks on them, are increasingly sophisticated. The proper incident detection, investigation, and analysis technology systems are essential to maximizing the skills of your security staff, implementing the proper processes, and learning from past attacks to respond more effectively.

- **Tip 7: Institute or improve formalized incident response tracking/workflow.** Too many organizations rely on a manual, decentralized system for tracking security incidents. Often this consists of little more than spreadsheets updated by individual analysts. Since some analysts may be more skilled or diligent than others at such updates, it can be very difficult to provide governance or properly track how incidents are being handled, and whether the process is improving over time.

A more effective system should be highly customizable to drive the organization’s incident response process from alert collection to incident creation and escalation through triage containment, analysis and remediation. Such a tool should integrate with other security platforms such as SIEM, AV, IDS and network monitoring to automatically create tickets based on alerts from them.

It should also allow the organization to apply custom prioritization/severity ratings to incidents, and to enrich tickets with internal data such as asset information and criticality ratings, as well as external data such as domain and blacklist information. The tool should also allow the organization to adjust the priority ratings based on new data about risks and vulnerabilities.
• **Tip 8: Employ centralized or real-time monitoring/alerting covering major portions of the enterprise.** To better detect and more efficiently investigate activities and alerts, security analysts need comprehensive and immediate visibility into key indicators of compromise. Besides network level telemetry, analysts need visibility into logs and events from underlying infrastructure, applications, and security systems. Finally, when dealing with malware, immediate visibility into what is happening on particular hosts also often proves to be critical. Such tools should, for example, be able to detect code injection, kernel hooking and system modification, as well as other techniques common to targeted attacks.

Among the requirements for providing this visibility are:

• An integrated platform for detection, investigation, management, and response.

• Comprehensive network packet-level monitoring on all Internet egress points and key internal network segments.

• Widespread log/event collection closely integrated with network-level visibility.

• File monitoring for behavior analysis and anomaly detection to highlight malware and endpoint anomalies, rather than relying on often outdated signature-based defense mechanisms.

• Continuous feeds of threat intelligence and indicators of compromise to accelerate the detection and investigation of threats.

• **Tip 9: Improve forensic analysis.** You can’t fight what you can’t see and understand. Understanding attacks requires deep-dive analysis using host/network/log level visibility combined with multiple forms of analytics, threat intelligence, and business and technical context.

Forensic tools for static and dynamic analysis can address many of these requirements. Such tools must be easily deployable throughout the IT infrastructure and be able to quickly connect to endpoints on demand. They should provide centralized access/visibility to the root causes of incidents, while minimizing system and memory burden. They must provide rapid and efficient assessment of the security incident, quickly identifying suspicious processes and files through the analysis of memory usage, open network connections, running processes, event logs of interest, and registry of hives/keys of interest.

Another important feature is a scriptable interface that allows users to automatically collect and analyze artifacts such as files, executables and DLLs, as well as screenshots and data from other systems and utilities, aggregating all the needed data within a “single pane of glass.”

• **Tip 10: Develop or improve cyber threat intelligence.** To move beyond simply reacting to new threats, organizations need an early warning system so they can take appropriate actions against even the most sophisticated threats.

Cyber Threat Intelligence (CTI) is the ability to aggregate and share private (e.g. subscription-based), peer (e.g. ISACA, FS-ISAC), public (e.g. US-CERT) and in-house threat information (e.g. e-mail and web operations) to identify potential threats more quickly. Organizations that are active in intelligence sharing between Open Source Intelligence (OSINT), industry partners and/or paid subscription services can create trending and threat actor profiles containing attack tactics, tools, delivery methods and command and control (C2) domains, among other details.
Creating a searchable central location (often referred to as a threat intelligence portal) ensures that analysts have access to the latest information and intelligence available. Automated integration of this portal with perimeter security tools allows instant alerts to analysts of indicators that match known threats.

FROM FIREFIGHTER TO STRATEGIC PARTNER

As security breaches cause massive damage to organizations’ reputations and bottom lines, CEOs and boards expect more than heroic ad-hoc security efforts. They demand consistent, measurable improvements in security response over time. They are also insisting on fine-tuned people, processes and technology that can limit the damage quickly when a security incident occurs.

Improving an organization’s security response requires a more formal, disciplined approach to everything from training to incident reporting, as well as more centralized and integrated tracking and analysis systems. But getting ahead of, rather than just responding to, security threats turns the security staff from reactive first responders to strategic partners in the long-term health of the enterprise.

This paper has been collectively written by RSA experts and practitioners from the global RSA Advanced Cyber Defense (ACD) Practice, including:

Shakeel Ahmad, Senior Consultant (EMEA), RSA ACD Practice
Azeem Aleem, Practice Lead (EMEA), RSA ACD Practice
Chris Bates, Advisory Consultant (Americas), RSA ACD Practice
Tadhg Cross, Global Manager – Operations, RSA ACD Practice
Matthew Gardiner, Senior Manager, RSA
Justin Grosfelt, Advisory Consultant (Americas), RSA ACD Practice
Sarah Kahler, Senior Manager, Consulting Operations, RSA ACD Practice
Stephen McCombie, Practice Lead/Senior Manager (APJ), RSA ACD Practice
Demetrio Milea, Advisory Consultant (EMEA), RSA ACD Practice
Charles Moisakis, Practice Lead (Americas), RSA ACD Practice
Andrew Slavkovic, Senior Consultant (APJ), RSA ACD Practice
Walter Tierney, Associate Consultant – Training/Education (Americas), RSA ACD Practice
Peter Tran, Senior Director, RSA ACD Practice
ABOUT THE RSA ADVANCED CYBER DEFENSE PRACTICE:

The RSA Advanced Cyber Defense Practice provides services that unify an organization’s security strategy, operations, and technology deployments and produce an actionable security-improvement plan that enables it to prioritize requirements and enhance its security posture. Enterprises can accelerate the detection, investigation, and remediation of security incidents and vulnerabilities; enhance the control they have over sensitive systems and IP; and gain a partner able to support the evolution of cyber-security initiatives. These services include a rapid breach-response service and an SLA-based retainer service providing surge access to resources and expertise. The RSA Advanced Cyber Defense Practice provides access to highly skilled, real-world security practitioners each with an average of 10-plus years of providing breach-management services and of building, operating, and managing SOCs. For more information about how your organization can improve incident readiness, response and resiliency visit rsa.im/ACDpractice.

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of intelligence-driven security solutions. RSA helps the world’s leading organizations solve their most complex and sensitive security challenges: managing organizational risk, safeguarding mobile access and collaboration, preventing online fraud, and defending against advanced threats. RSA delivers agile controls for identity assurance, fraud detection, and data protection, robust Security Analytics and industry-leading GRC capabilities, and expert consulting and advisory services. For more information, please visit www.RSA.com.

EMC®, EMC, the EMC logo, RSA, and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries.

© Copyright 2014 EMC Corporation. All rights reserved.

www.rsa.com

H13297